2.1 Evaluation of Defense-in-Depth Attributes and Safety Margins

One aspect of the engineering evaluation is to show that the proposed change does not compromise the fundamental safety principles on which the plant design was based. Design-basis accidents (DBAs) play a central role in the design of nuclear power plants. DBAs are a combination of postulated challenges and failure events against which plants are designed to ensure adequate and safe plant response. During the design process, plant response and associated safety margins are evaluated using assumptions of physical properties and operating characteristics that are intended to be conservative. National standards and other considerations such as defense-in-depth attributes and the single-failure criterion constitute additional engineering considerations that also influence plant design and operation. The licensee's proposed LB change may affect margins and defenses incorporated into the current plant design and operation; therefore, the licensee should reevaluate the safety margins and layers of defense to support a requested LB change. As part of this evaluation, the impact of the proposed LB change on the functional capability, reliability, and availability of affected equipment should be determined. The plant's LB identified in the FSAR is the reference point for judging whether a proposed change adversely affects safety margins or defense in depth. Sections 2.1.1 and 2.1.2 below provide guidance on assessing whether implementation of the proposed change maintains adequate safety margins and consistency with the defense-in-depth philosophy.

2.1.1 *Defense-in-Depth*

The engineering evaluation should evaluate whether the impact of the proposed LB change is consistent with the defense-in-depth philosophy. In this regard, the intent of this principle is to ensure that the philosophy of defense-in-depth is maintained, not to prevent changes in the way defense-in-depth is achieved. This section provides some background on the defense-in-depth philosophy. Next is discussion of seven key factors that may be used to evaluate the impact of a proposed change on defense in depth. Finally, this section provides guidance on a process for evaluating the seven key factors.

2.1.1.1 Background

Defense in depth is an element of the NRC's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility[1]. The defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions and prevent the release of radioactive material. It has been and continues to be an effective way to account for uncertainties in equipment and human performance and, in particular, to account for the potential for unknown and unforeseen failure mechanisms or phenomena, which (because they are unknown or unforeseen) are not reflected in either the PRA or traditional engineering analyses.

At a high level, nuclear power plant defense in depth includes the following successive measures: (1) robust plant design to survive hazards and minimize challenges that could result in an event occurring; (2) prevention of a severe accident (core damage) should an event occur; (3) confinement or containment of the source term should a severe accident occur; and (4) protection of the public from any releases of radioactive material (through, e.g., siting in low population areas and the ability to shelter or evacuate people if necessary). It is convenient to think about these successive measures as *layers* of defense between the radioactive source term and the public.

---

[1] Staff Requirements Memorandum (SRM) - SECY-98-0144, "White Paper on Risk-Informed and Performance-Based Regulation," March 1, 1999, (Agencywide Document Access and Management System (ADAMS) accession number ML003753601)

If a comprehensive risk analysis is done, it can provide insights into whether the extent of defense in depth (e.g., balance among core damage prevention, containment failure, and consequence mitigation) is appropriate to ensure protection of public health and safety. However, to address the unknown and unforeseen failure mechanisms or phenomena, traditional defense in depth considerations should be used or maintained.

2.1.1.2 Key Factors for Evaluating the Impact of LB Changes on Defense in Depth

Any one or more of the four layers of defense discussed above may be adversely impacted by a proposed change to a plant's licensing basis. However, there are no objective criteria or quantitative decision criteria for assessing the impact. Therefore, the NRC has identified seven factors that should be used to qualitatively assess the impact of the change on defense in depth. Some of these factors are high level (e.g., balance among core damage, containment failure, and consequence mitigation), whereas other factors are at a more detailed level and could apply to any of the layers of defense (e.g., defenses against human error). Applying these factors is discussed in more detail in section 2.1.1.3.

The NRC finds it acceptable for a licensee to use the following seven key factors to evaluate whether a proposed change to the LB maintains the philosophy of defense in depth.

1. Preserve a reasonable balance among the four layers of defense.

   A reasonable balance of the four layers of defense - minimizing challenges to the plant, preventing any events from progressing to core damage, containing the radioactive source term, and emergency preparedness) helps to ensure an apportionment of the plant's capabilities between limiting disturbances to the plant and mitigating their consequences. "Reasonable balance" is not meant to imply an equal apportionment of capabilities. A reasonable balance is preserved if the proposed plant change does not significantly reduce the effectiveness of a layer that exists in the plant design before the proposed change. The NRC recognizes that there may be aspects of a plant's design that may cause one of the four layers to be adversely affected. For these situations, the balance between the other three layers becomes especially important when evaluating the impact of a proposed change to the LB and its impact on defense in depth.

2. Preserve adequate capability of design features without an over-reliance on programmatic activities as compensatory measures.

   Programmatic activities are used to ensure safety functions; however, the regulations demonstrate a definite preference for engineered safety features to mitigate DBAs. The licensee should adhere to this preference and, therefore, should assess whether the proposed change would increase the need for programmatic activities to compensate for the lack of engineered features. If the change requires new or additional reliance on administrative controls, the licensee should justify that reliance on these measures is not excessive. Use of compensatory measures may be considered overreliance when a programmatic activity is substituted for an engineered means of performing a safety function, or failure of the programmatic activity could prevent an engineered safety feature from performing its intended function. Moreover, overreliance on a programmatic activity can potentially result in significant reduction in the effectiveness of one of the defense-in-depth layers that exists in the plant design before the proposed change, or it may lessen the effectiveness of one of the fission product barriers. The licensee should evaluate the impact to confirm that a reasonable balance of the defense-in-depth layers is preserved.

   The NRC also recognizes that programmatic activities used as compensatory measures are sometimes associated with temporary conditions. A licensee may request a risk-informed change

to the plant's licensing basis to permit occasional entry into conditions requiring compensatory measures. For such situations, the licensee should demonstrate that the plant condition requiring such compensatory measures would occur at a sufficiently low frequency.

3. Preserve sufficient system redundancy, independence, and diversity.

The importance of system redundancy, independence and diversity is to ensure that the "safety functions" can be achieved. The safety functions are accomplished by the safety related structures, systems, and components those functions needed to shut down the reactor, remove the residual heat, and contain any radioactive material release.[2] 10 CFR Part 50, Appendix A, General Design Criteria discusses the need for system redundancy, independence and diversity specifically as a means to prevent a single failure; that is, the system safety function can be accomplished assuming a single failure[3]. Redundancy provides for duplicate equipment that enables the failure or unavailability of at least one set of equipment to be tolerated without loss of function. Independence among equipment implies that the redundant equipment are separate such that they do not rely on the same supports to function. It can sometimes be achieved by the use of physical separation or physical protection. Diversity is accomplished by having equipment that perform the same function rely on different attributes, such as different principles of operation, different physical variables, different conditions of operation, or production by different manufacturers.

A substantial reduction in the ability to accomplish a safety function is not consistent with the defense-in-depth philosophy. A safety function may be compromised if one of the plant features that provides for either system redundancy, independence, or diversity is defeated. This adverse impact could occur by the introduction of a new dependency that could potentially defeat the redundancy, independence or diversity of the affected equipment. That is, system redundancy, independence and diversity can be assumed to be sufficient if, given the proposed licensing change, the affected system safety function can be accomplished assuming a single failure.

The licensee should demonstrate that the proposed licensing change would not affect system redundancy, independence, or diversity of the affected equipment; that is, the affected system safety function can still be accomplished assuming a single failure.

4. Preserve adequate defense against potential common-cause failures (CCF) and assess the potential for the introduction of new common-cause failure mechanisms.

---

[2] 10 CFR 50.2 defines safety-related as systems and components means those structures, systems and components that are relied upon to remain functional during and following design basis events to assure:
(1) The integrity of the reactor coolant pressure boundary
(2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
(3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable.

[3] A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety function. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions. [10 CFR 50, Appendix A, General Design Criteria for Nuclear Power Plants, Definitions]

An important aspect of ensuring defense in depth is to guard against CCF. Failure of several devices or components to function may occur as a result of a single specific event or cause. Such failures may simultaneously affect several different items important to risk. The event or cause may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a natural phenomenon, a human-induced event, or an unintended cascading effect from any other operation or failure within the plant. A CCF can result in the failure, degradation, or effectiveness of a defense-in-depth layer that exists in the plant design before the proposed change.

The licensee should evaluate the proposed change to determine whether it increases the potential for events or causes that would be a CCF. The licensee should also evaluate the proposed change to determine whether new CCF mechanisms could be introduced.

5. Maintain integrity of multiple fission product barriers.

In this context a fission product *barrier* is a physical structure between the source term and the public, which is intended to prevent a release of radionuclide material. This factor includes physical barriers (e.g., the reactor coolant system pressure boundary) and the systems and components that protect the integrity of physical barriers (e.g., emergency core cooling system). The effectiveness of barriers is reduced if multiple barriers can be defeated or degraded by a single event as a result of the proposed change.

To maintain the integrity of multiple barriers, the licensee should ensure that the change does not result in a new event or increase the likelihood of an existing event whose effects would disable multiple barriers that are relied upon to mitigate the consequences of the initiating event.

6. Preserve sufficient defense against human errors.

Human errors include (1) the failure of operators to perform the actions necessary to operate the plant or respond to off-normal conditions and accidents, (2) errors committed during test and maintenance, and (3) operators performing an incorrect action. The plant design and operation includes defenses to prevent the occurrence of such events and errors. These defenses generally involve the use of procedures, training, and human engineering. These defenses are preserved if the proposed plant change does not increase the potential for human errors that can lead directly to a beyond-design-basis event or affect the ability of operators to place the plant in a safe-shutdown condition or carry out emergency operating procedures correctly. Human errors can result in the degradation or failure of a system to perform its function, thereby significantly reducing the effectiveness of one of the defense-in-depth layers or one of the fission product barriers.

The licensee should assess whether the proposed change would create new operator actions, increase the burden on operators in responding to events, or increase the probability of existing operator errors. The licensee should consider whether the change creates new situations that are likely to cause errors, not only for operators, but for maintenance personnel and other plant staff.

7. Maintain the intent of the plant's design criteria.

The plant's design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for SSCs important to safety; that is, SSCs that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the

public. When evaluating the effect of the proposed change, the licensee should determine whether the plant's design criteria are affected.

The plant's design criteria define requirements that implement the defense-in-depth philosophy; as a consequence, a compromise to those design criteria can directly result in a significant reduction in the effectiveness of one of the defense-in-depth layers.